ATM 해킹 위협과 보안 전망

소프트포럼 보안기술분석팀
박찬암 (팀장) / 2010. 07. 30

개요

2010년 7월, 매년 미국에서 개최되는 세계 최대 보안 컨퍼런스인 BlackHat에서 현금 자동 입출금기(Automated Teller Machine, 이하 ATM) 상의 취약성을 이용하여 마치 잭팟을 터뜨린 것처럼 현금이 원하는 만큼 자유롭게 인출되도록 하는 기술이 시연 및 공개되었다. 해당 이슈는 BlackHat에서 단연 가장 최고의 이슈로 부각되었으며, 각종 언론을 통해 위험의 심각성도 크게 부각되어 알려졌다. 기사에서 발표자가 언급한 내용에 따르면, 이제까지 보았던 모든 ATM에서 현금 인출이 원하는 만큼 가능한 취약성이 존재하고 있다고 한다. 본 문서에서는 이러한 취약성에 대한 전반적인 내용 및 전망 등을 살펴볼 것이다. 하지만 아쉽게도, BlackHat에서 발표된 수많은 내용들 중 이에 대한 발표 자료만 공개되지 않았기 때문에 약간의 제약이 있음을 밝혀둔다.

목차

1. ATM 보안 취약성 개요

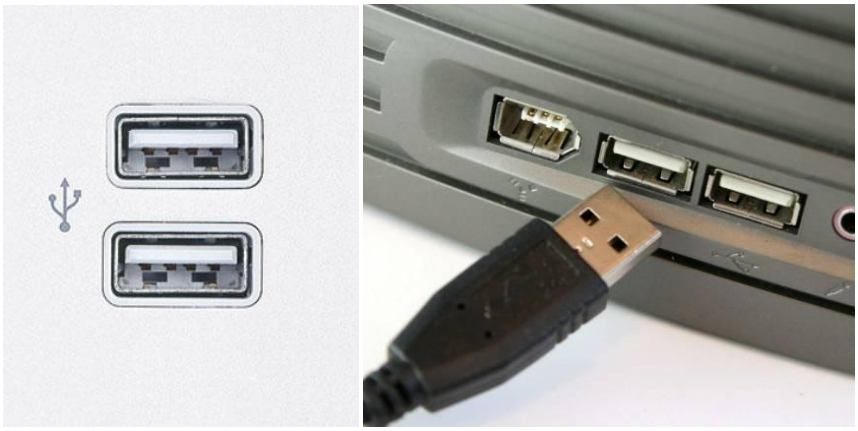
Las Vegas에서 개최된 BlackHat 2010의 최대 화제였던 ATM 해킹은 Jackpotting(잭팟팅)이라는 제목으로 해외 보안 업체 IOActive의 연구원에 의해 발표되었다. 발표자에 따르면, ATM의 보안 위협에 대한 내용을 다루는 것이 목적이고 "ATM 해킹법"이 본 의도가 아니기 때문에 상세한 기술은 설명하지 않는다고 한다. 하지만, 개략적인 설명 내용을 통해 대부분의 기술 유추가 가능하였다.
ATM 해킹을 위해서는 총 두 가지 방법론으로 접근이 가능한데, 첫 번째는 물리적인 보안 위협과 소프트웨어적인 보안 위협을 합친 공격이며 두 번째는 원격 접근을 통한 공격이다.
대부분의 ATM은 윈도우 기반(정확히는 Windows CE)에서 구동되기 때문에 시연에 사용되었던 공격 코드는 윈도우 프로그램으로 작성되어있다.

2. ATM 공격 기술 (1)

우선 물리적인 취약성과 소프트웨어적인 취약성이 복합된 공격 방법을 알아보았다. 순서는 다음과 같다.

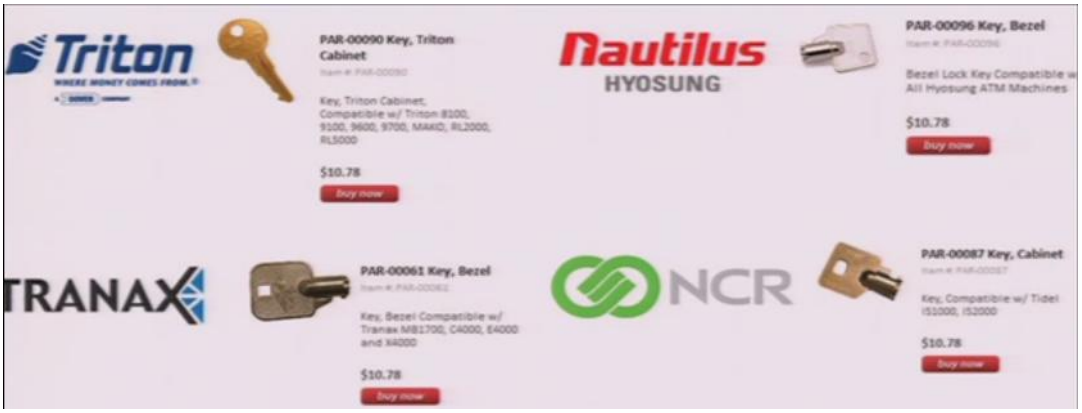
1. 물리적인 취약성을 이용한 공격
2. 소프트웨어적인 취약성을 이용한 공격
3. Jackpotting(현금을 원하는 만큼 인출)

1번의 공격은 일반적으로 디바이스(ATM, 교통카드 단말, 지문 인식기 등)를 제어하기 위하여 존재하는 USB 포트에 접근하기 위한 공략과정이다. 이러한 디바이스도 결국은 일종의 중소형 컴퓨터와 같기 때문에 제어를 위해서는 별도의 USB 포트 등을 통하여 노트북에 연결하는 방식이 주로 사용된다.



<그림 1> 일반적인 USB 포트

그런데 ATM의 경우, 현금을 다루는 민감한 기기이기 때문에 접근 제한의 목적으로 이러한 USB 포트를 이용하려면 별도의 열쇠를 이용해서 잠겨있는 특정 부분을 열어야 한다. 이것이 첫 번째로 언급했던 물리적인 취약성을 공략하는 내용이다.
잠겨있는 USB 포트를 사용하기 위한 방법은 다양하겠지만(물리적인 파괴 등), 발표자가 제시한 가장 무난하면서도 세련된 접근법은 따로 있다. 바로, ATM에서 사용되는 열쇠가 인터넷 등에서도 쉽게 구할 수 있다는 점을 악용하여 손 쉽게 열쇠를 구해서 잠겨있는 부분을 열면 해결된다.



<그림 2> 인터넷에서 쉽게 구할 수 있는 ATM 열쇠

이렇게 USB에 접근하게 되면 공격을 위해 일차적으로 이루어지는 물리적 취약성을 이용한 공략이 끝나게 된다.
두 번째 소프트웨어적인 취약성을 이용한 공격(2번)이 남아있는데, 상세한 기술적 접근이 아닌 큰 틀에서의 방법론적 측면에서 바라보면 이 또한 상당히 간단하게 설명될 수 있다.
ATM에 존재하는 포트에 USB를 꼽게 되면 자동으로 USB에 저장된 프로그램이 실행되는 문제점을 이용한 것이다. 그래서 공격자는 미리 제작된 악성 프로그램을 USB에 저장해둔 뒤, 해당 포트에 연결하면 자동으로 악성 프로그램이 실행되어 ATM을 장악 할 수 있게 된다. 1장에서 언급했던 것과 같이 이를 위한 악성 코드는 Windows CE 기반 즉, 윈도우 기반에서 제작되었다.
결국 현금 인출과 같은 작업들도 윈도우에서 동작하는 프로그램에 의해서 이루어지는 것이기 때문에 이렇게 ATM을 장악하게 되면 최종 목표인 현금을 원하는 만큼 인출하는 Jackpotting도 가능하게 된다.

3. ATM 공격 기술 (2)

이번 장에서 설명하는 기술도 ATM에 악성 프로그램을 실행하도록 하여 현금을 인출하는 방식에서는 이전 장과 다른 부분이 없다. 다만 첫 번째 공격 기술과의 차이는, ATM에서 악성 프로그램을 실행하기 위한 "접근 방식"이라고 볼 수 있다. 즉, 어떠한 방법으로 ATM에 원하는 프로그램을 실행 할 수 있는가에 대한 접근 방식이 다르다는 부분 이외에는 이전의 내용과 동일하다.
간단하게 설명하면, ATM에도 원격에서의 관리를 위한 일종의 관리자 페이지가 존재하는데, 주로 인터넷이나 전화를 통해 접근이 가능하다고 한다. 하지만, 이에 대한 보안 수준이 상당히 낮기 때

문에 특별히 고 난이도의 기술 없이도 손쉽게 인증 우회를 할 수 있게 되는 것이다. 이렇게 인증 우회를 거치게 되면 ATM에 대한 다양한 정보와 함께 공격자의 목적인 악의적인 프로그램의 실행도 가능하게 된다. 이후의 작업은 이전과 동일하므로 생략하도록 한다.

4. ATM 취약성 방어 기술

결론적으로 보면, 이번 BlackHat에서 소개된 ATM 해킹 기술은 크게 두 가지 취약성으로 인해 발생한 것으로 볼 수 있다. 하나는, 물리적으로 견고한 잠금 체계를 갖추지 못하고 해당 열쇠를 시중에서 쉽게 구해 잠금 장치를 풀고 USB 포트 접근이 가능하다는 것이고, 다른 하나는 악성 프로그램의 무분별한 실행에 대한 대응책이 없다는 것이다. ATM과 같이 제한적인 기능을 수행하는 디바이스의 경우 윈도우의 아주 일부 기능(ATM 프로그램 구동)만이 필요하기 때문에 그러한 특성에 커스터마이징 된 보안 대처가 필요하다고 볼 수 있다.
발표자도 이러한 취약성을 막기 위해서는 물리적인 잠금 장치의 업그레이드와 운영체제의 실행파일 서명(Executable Signing)을 해야 한다고 언급하였다. 여기서 실행파일 서명이란, ATM의 경우 사용하는 프로그램이 한정적이어서 외부 프로그램을 사용하는 일이 거의 없기 때문에 이러한 부분을 고려하여 안전하다고 서명된 프로그램만 ATM에서 사용 할 수 있도록 제한하는 것을 뜻한다.

5. ATM 보안 기술 전망

이번과 같은 취약성으로 볼 때 향후 가장 기대되는 ATM 보안 기술은 "실행파일 서명"과 관련된 솔루션 등으로 생각된다. 물리적으로 USB를 통해 접근하여 원하는 프로그램을 실행시키는 방법 이외에도, ATM이 어떤 식으로든 직간접적으로 인터넷 망에 연결되어 있기 때문에 온라인상의 경로를 통한 해킹 위협에 100% 안전하다고 장담할 수 없으며 내부 위협도 간과하기 힘들다. 그렇기 때문에 실행파일 서명을 통하여 신뢰성이 검증된 프로그램만을 ATM에서 동작하도록 한다면 외부에서 유입되는 악의적인 프로그램의 무분별한 실행을 막을 수 있을 것이다.
국내에서도 2009년 12월경 이즈넷이라는 회사에서 ATM 보안 솔루션에 대한 필요성 및 자사 제품 홍보를 위한 기사를 냈었는데(참고자료 [2]), 그러한 솔루션을 이미 도입한 은행권도 있지만 아직까지 인터넷 뱅킹 보안 솔루션과 같이 필수적인 요소로 자리잡고 있지는 않고 있는 것으로 보인다.
이번 ATM 해킹 이슈를 계기로 금융권이 보안에 대한 경각심을 가지고 정책적으로 반영이 된다면 솔루션 도입 및 그로 인한 ATM의 보안성이 더욱 강화될 것이라 기대해본다.

참고자료

[1] Armed with exploits, ATM hacker hits the jackpot
http://www.theregister.co.uk/2010/07/28/atm_hacking_demo/

[2] "ATM 전용 보안솔루션 필요" - 이즈넷, 일부 금융권 도입미뤄 정보유출 등 문제제기
http://www.dt.co.kr/contents.html?article_no=2009120402010151745002